

# Our Commitment to Cyber Security

As a business, we recognize the importance of protecting sensitive data and ensuring a secure operational environment. We have taken significant steps to enhance our security posture. While our certification is in progress, we are already implementing best practices to safeguard your data in multiple disciplines on our hybrid environment.

## ACCESS CONTROL

**Technical security:** we have network- and host-based intrusion prevention systems to protect our infrastructure from threats.

**Multi-Factor Authentication:** MFA for everyone, to add an extra layer of security for user accounts and provide auditing records.

## DATA PROTECTION AND BACKUP

**Multi-tier backups:** we backup our sensitive data, on-premise and on cloud, via multiple techniques and test our restore procedure after every backup, providing robust redundancy and quick recovery.

**Least privilege principle:** we make sure that everybody has access to only the data and tools they are supposed to have.

## REDUNDANCY AND CONTINUITY

**Redundant Resources:** We maintain redundant resources (like internet connection) to minimize downtime and ensure high availability.

**Security audits:** we are driven to continuously improve our security posture, which is why we contract third parties to assess our security.

## NETWORK SECURITY

**Firewall Protection:** Advanced firewall systems are in place to protect our network from unauthorized access.

**Intrusion Detection Systems:** We use IDS to monitor and detect suspicious activities within our network and automatically map all connected devices.

## SOFTWARE SECURITY

**Regular Updates:** We use automated tooling to keep our software dependencies up to date and review them for known vulnerabilities.

**Change Tracking:** We document the changes we make on our production code with a clear versioning scheme on each software artifact and track the changes both in component changelogs and link them back to our project management tools.

## COMPLIANCE AND STANDARDS

**ISO 9001 Certification:** Our ISO 9001 certification demonstrates our commitment to quality management, which indirectly supports our cyber security efforts.

**Preparation for ISO 27001:** We are actively working towards ISO 27001 certification, ensuring our practices align with international standards for information security.

## EMPLOYEE TRAINING

**Phishing Simulations:** We run phishing simulations to help employees recognize and respond to phishing attempts.